IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) In an interactive system for managing **[[**access**]]** entry to a secured Location via a communications network, the system comprising in combination:

an entry control Device assigned for use in gaining entry to said Location by a Device-User;

a plurality of databases, each of said databases requiring a different level of access;

Software configured to require a password from each of a plurality of Database-Users corresponding to one of said levels of access; and

said Software operable to perform one or more functions including at least one of adding, modifying, deleting and viewing entries in said databases, said functions selectable by each said Database-User according to said Database-User's password.

2. (Previously Presented) In a system according to claim 1 wherein said Devices are tangible items containing encoded criteria.

3 (Previously Presented) In a system according to claim 2 wherein said encoded criteria are assigned to each said Device-User.

4. (Original) In a system according to claim 2 wherein said tangible items are selected from the group consisting of a key, access card, chip and bar codes.

5. (Previously Presented) In a system according to claim 1 wherein said Devices are intangible objects assigned to and in possession of each said Device-User.

6. (Original) In a system according to claim 5 wherein said objects are selected from the group consisting of code numbers, PIN numbers and code words or phrases.

7. (Currently Amended) In a system according to claim 1 wherein said Location includes an accessway having a locking member which must be unlocked to gain **[[**access**]]** entry to said Location.

8. (Previously Presented) In a system according to claim 6 wherein said Location includes a security system which requires one of said objects to gain access to information in said security system.

9. (Original) In a system according to claim 1 wherein one of said different levels of access is selected from the group consisting of a key, card and padlock combination.

10. (Previously Presented) In a system according to claim 1 wherein one of said different levels of access includes the ability to configure said Device for said Location.

11. (Currently Amended) In a system according to claim 1 wherein one of said different levels of access includes the ability to determine which of said Device-Users is allowed **[[**access**]]** entry to one of said secured Locations.

12. (Previously Presented) In a system according to claim 1 wherein said functions include adding, modifying, deleting and viewing entries from said plurality of said databases.

13. (Previously Presented) In a system according to claim 12 wherein a profile is provided to control access of each said Database-User to said database entries.

14. (Currently Amended) In an interactive system for managing **[[**access**]]** entry to one or more secured Locations via a communications network, the system comprising in combination:

an entry control Device assigned to each of said one or more Locations for use in gaining entry to said one or more Locations by a Device-User;

a plurality of databases whereby each of said databases has a different level of access;

Software configured to require a password from each of a plurality of Database-Users corresponding to one of said levels of access; and

wherein real time data is maintained in said databases on the status of each said Device, one or more Locations, Device-User and Database-Users.

15. (Previously Presented) In an interactive system according to claim 14 wherein said Database-Users are also Device-Users and are each assigned one of said passwords to enable entry to said one or more Locations and to define said level of access to said data.

16. (Previously Presented) In a system according to claim 14 wherein said Devices are tangible items containing encoded criteria, said encoded criteria being assigned to each said Device-User, and said tangible items being selected from the group consisting of a key, access card, chip and bar codes.

17. (Previously Presented) In a system according to claim 14 wherein said Devices are intangible objects assigned to and in possession of each said Device-User, and said objects are selected from the group consisting of code numbers, PIN numbers and code words or phrases.

18. (Currently Amended) In a system according to claim 14 wherein each said secured Location includes an accessway having a locking device which must be unlocked to gain **[[**access**]]** entry to said secured Location, and said secured Location includes a security system which requires one of said Devices to gain access to information in said security system.

19. (Original) In a system according to claim 14 wherein one of said different levels of access is selected from the group consisting of a key, card and padlock combination.

20. (Previously Presented) In a system according to claim 15 wherein one of said different levels of access includes the ability to configure each said Device for said one or more secured Locations.

21. (Previously Presented) In a system according to claim 15 wherein one of said different levels of access includes the ability to determine which of said Device-Users is allowed access to said one or more secured Locations.

22. (Previously Presented) In a system according to claim 15 wherein said Software is configured to allow said Database-Users to perform functions include adding, modifying, deleting and viewing entries from each of said databases according to the Database-User's level of access.

23. (Previously Presented) In a system according to claim 14 further comprising access control means for controlling access of each said Database-User to said databases according to the Database-User's password.

24. (Previously Presented) In a system according to claim 23 wherein said access control means is operative to display records of said data on the status of each of said Devices for said one or more secured Locations and to display information pertaining to ownership and other associated data for each of said Devices.

25. (Previously Presented) In a system according to claim 24 wherein said access control means is operative to display information relating to one of said Devices which is lost or stolen.

26. Canceled.

27. Canceled.

28. (Previously Presented) A method for managing access by one or more Device-Users to an access control system for at least one secured Location comprising:

assigning an entry control Device to said Location for use in gaining entry to said Location by each said Device-User;

providing at least one database defining different levels of accessible data by a plurality of Database-Users, said data relating to said Location, Device, Device-Users or Database-Users;

assigning a password to each said Database-User which corresponds to one of said levels; and

providing one or more functions selected by said Database-User from the group consisting of adding, modifying, deleting and viewing data entries in said at least one database.

29. (Previously Presented) The method according to claim 28 further comprising:

interactively communicating between each said Database-User and said at least one database.

30. (Previously Presented) The method according to claim 28 further comprising:

maintaining data on said Devices, Locations, and Device-Users in said at least one database in a real time mode.

31. (Currently Amended) A method for managing access by one or more Users to an access control system for at least one secured Location comprising the steps of:

assigning an entry control Device to said Location for use in gaining **[[**access**]]** entry by each said User;

providing a plurality of databases wherein each of said databases defines a different level of access to said Location or to data relating to said Location;

assigning a password to each said User which corresponds to one of said levels; and

providing one or more functions in each of said databases from which each said User can select;

wherein said functions include the steps of adding, modifying, deleting and viewing data entries from each of said databases.

32. (Currently Amended) A method for managing access by one or more Users to an access control system for at least one secured Location comprising the steps of:

assigning an entry control Device to said Location for use in gaining **[[**access**]]** entry by each said User;

providing a plurality of databases wherein each of said databases defines a different level of access to said Location or to data relating to said Location;

assigning a password to each said User which corresponds to one of said levels;

providing one or more functions in each of said databases from which each said User can select; and

dynamically linking said databases and said User via a communications network.

33. (Previously Presented) The method according to claim 32 further comprising:

maintaining current and historical data on each said Device, Location, and User.

34. (Previously Presented) The method according to claim 32 further comprising:

verifying that the function selected by one of said Users is authorized.

35. (Previously Presented) The method according to claim 28 further comprising:

looking up in said at least one database to determine if said User is authorized to have access to one of said levels of access.

36. (Previously Presented) The method according to claim 28 further comprising:

providing information relating to a Device which has been found.

37. (Previously Presented) The method according to claim 28 further comprising:

providing information relating to a Device which has been lost or stolen.

38. Canceled.

39. Canceled.

40. (Previously Presented) The method according to claim 28 further comprising:

adding one of said Devices, Locations and Users to said at least one databases.

41. (Currently Amended) A method for managing access by one or more Users to an access control system for at least one secured Location comprising:

assigning an entry control Device to said Location for use in gaining **[[**access**]]** entry by each said User;

providing a plurality of databases wherein each of said databases defines a different level of access to said Location or to data relating to said Location;

assigning a password to each said User which corresponds to one of said levels;

providing one or more functions in each of said databases from which each said User can select; and

recording the addition of a key blank in one of said plurality of databases.

42. (Previously Presented) The method according to claim 28 further comprising:

ordering one of said Devices.

43. (Currently Amended) A method for managing access by one or more Users to an access control system for at least one secured Location comprising:

assigning an entry control Device to said Location for use in gaining **[[**access**]]** entry by each said User;

providing a plurality of databases wherein each of said databases defines a different level of access to said Location or to data relating to said Location;

assigning a password to each said User which corresponds to one of said levels;

providing one or more functions in each of said databases from which each said User can select; and

adding an additional access control system to said plurality of databases.

44. (Currently Amended) In an interactive system for managing **[[**access**]]** entry to a secured Location through an entry control Device used by a Device-User, said system being accessible by a Database-User operating through a communications network, the system comprising:

at least one database, said at least one database requiring a different level of access for different types of data stored in said at least one database;

Software configured to require a password from said Database-User corresponding to one of said levels of access; and

said Software allowing one or more functions including at least one of adding, modifying, deleting and viewing data in said at least one database, said functions selectable by each said Database-User according to said Database-User's password.

45. (Previously Presented) In a system according to claim 44 wherein said Software is configured to require a multi-level password from said Database-User.